Billing Code 4710-24

DEPARTMENT OF STATE

[Public Notice: 11631]

Privacy Act of 1974; System of Records

ACTION: Notice of a modified system of records.

SUMMARY: The information collected and maintained in Integrated Logistics Management Records is necessary to: 1) ensure fiscal accountability in issuing federal assistance, 2) coordinate the logistics of transporting the household effects of Department of State and other Embassy employees, and contracting services, 3) allow customers to submit and track requests for services, 4) allow service providers to fulfill and track customer requests, and 5) fulfill International Cooperative Administrative Support Services (ICASS).

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this system of records notice is effective upon publication, with the exception of the routine uses that are subject to a 30 day period during which interested persons may submit comments to the Department. Please submit any comments by March 1st 2022.

ADDRESSES: Questions can be submitted by mail, email, or by calling Eric F. Stein, the Senior Agency Official for Privacy on (202) 485-2051. If mail, please write to: U.S Department of State; Office of Global Information Systems, A/GIS; Room 1417, 2201 C St., N.W.; Washington, DC 20520. If email, please address the email to the Senior Agency Official for Privacy, Eric F. Stein, at Privacy@state.gov. Please write "Integrated Logistics Management Records, State-70" on the envelope or the subject line of your email.

FOR FURTHER INFORMATION CONTACT: Eric F. Stein, Senior Agency Official for Privacy; U.S. Department of State; Office of Global Information Services, A/GIS; Room 1417, 2201 C St., N.W.; Washington, DC 20520 or by

calling on (202) 485-2051.

SUPPLEMENTARY INFORMATION: The purpose of this modification is to make substantive and administrative changes to the previously published notice. This notice modifies the following sections: Summary, Dates, Addresses, For Further Information Contact, Supplementary Information, System Name and Number, System Location(s), Categories of Individuals Covered by the System, Categories of Records in the System, Routine Uses of Records Maintained in the System, Policies and Practices for Storage of Records, Policies and Practices for Retention and Disposal of Records, and Administrative, Technical, and Physical Safeguards. In addition, this notice makes administrative updates to the following sections: Policies and Procedures for Retrieval of Records, Record Access Procedures, Notification Procedures, and History. This notice is being modified to reflect the Department's move to the cloud, new OMB guidance, the use of contractors, new routine uses, updated contact information, and a notice publication history. The Categories of Individuals Covered by the System section has been expanded to include individuals applying for or receiving Federal assistance. The Categories of Records section has been expanded to account for additional records stored within Integrated Logistics Management Records to include Federal assistance applications and Federal assistance awards, personal service contract payment information, and documentation necessary to process invoices and claims for payment.

SYSTEM NAME AND NUMBER: Integrated Logistics Management Records, State-70.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION(S): (a) Department of State domestic data centers located within the U.S., with local infrastructure placed overseas at U.S. Embassies, U.S. Consulates General, and U.S. Consulates; and U.S. Missions, (b) within a government cloud platform provided by the Department's Enterprise Server Operations Center

(ESOC), 2201 C Street NW, Washington, DC 20520.

SYSTEM MANAGER(S): Managing Director, Program Management and Policy (A/LM/PMP); Department of State; 1800 N Kent Street; Arlington, VA 22209, reachable at A/LM Front Office, A-LMFrontOfficeAssistants@state.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 22 U.S.C. 4081, Travel and Related Expenses; 22 U.S.C. 5724, Travel and Transportation Expenses of Employees Transferred; 5 U.S.C. 301, 302, Management of the Department of State; 22 U.S.C. 2581, General Authority; 22 U.S.C. 2651a, Organization of the Department of State; 22 U.S.C. 2677, Availability of Funds for the Department of State; 22 U.S.C. 3921, Management of the Foreign Service; 22 U.S.C. 3927, Responsibility of Chief of Mission; E.O. 9397 (Numbering System for Federal Accounts Relating to Individual Persons); E.O. 9830 (as amended) (Amending the Civil Service Rules and Providing for Federal Personnel Administration); and E.O. 12107 (as amended) (Relating to the Civil Service Commission and Labor-Management in the Federal Service); 22 U.S.C. Chapter 52 Foreign Service; 31 U.S.C. 901—903 Agency Chief Financial Officers; Federal Financial Management Improvement Act of 1996.

PURPOSE(S) OF THE SYSTEM: The information contained in this system of records is collected and maintained by the Office of Logistics Management, Office of Program Management and Policy (A/LM/PMP) in the administration of its responsibility for providing worldwide logistics services and integrated support. The information collected and maintained in this system of records is necessary to: 1) ensure fiscal accountability in issuing federal assistance, 2) coordinate the logistics of transporting the household effects of Department of State and other Embassy employees, and contracting services, 3) allow customers to submit and track requests for services, 4) allow service providers to fulfill and track customer requests, and 5) to fulfill ICASS.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Current and

former Civil Service (CS) and Foreign Service (FS) employees of the Department of State (DOS) including members of the Senior Executive Service, Presidential appointees, employees under full-time, part-time, intermittent, temporary, and limited appointments; anyone serving in an advisory capacity (compensated and uncompensated); other agency employees on detail to the Department or stationed at U.S. Missions abroad who use DOS transportation services; former Foreign Service Reserve Officers; Presidential Management Interns, Foreign Affairs Fellowship Program Fellows, student interns and other student summer hires, Stay-in-School student employees, Cooperative Education Program participants, members of the public applying for or receiving Federal assistance; and eligible CS or FS family members. The Privacy Act defines an individual at 5 U.S.C. 552a (a)(2) as a United States citizen or lawful permanent resident.

CATEGORIES OF RECORDS IN THE SYSTEM: The system contains records about individuals related to procurement, property, logistics management, and Federal Assistance Awards. Specific types of records include:

a) Travel Authorizations (TAs) which contain name, date of birth, address, e-mail, phone, and the last four digits of the Social Security number (SSN).

b) Federal Assistance Applications and Federal Assistance Awards, which may include contact information including, but not limited to, applicant or recipient's name, address, telephone number, email address, and tax identification number.

c) Personal Service Contract payment information, which may include recipient's name, email address, and tax identification number.

d) Documentation necessary to process invoices and claims for payment, including employee information for reimbursement.

e) Information necessary to fill out service requests (*e.g.*, office services, technology support, travel and transportation, leasing property and maintenance services,

human resources, and security), which may contain business address, personal address, passport number, clearance, citizenship, and last 4 digits of SSN, scans of government-issued IDs (which may include driver's licenses or passport).

RECORD SOURCE CATEGORIES: These records contain information obtained primarily from the individual who is the subject of these records.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

The information in Integrated Logistics Management Records may be disclosed to the following:

(a.) Appropriate agencies, entities, and persons when (1) the Department of State suspects or has confirmed that there has been a breach of the system of records; (2) the Department of State has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department of State (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of State efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(b.) Another Federal agency or Federal entity, when the Department of State determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

(c.) Anyone who is under contract to the Department of State to fulfill an agency function but only to the extent necessary to fulfill that function.

(d.) Service providers to fulfill ICASS services at post or logistics service requests domestically. Service providers may include Department of State employees, locally employed staff at post, private service vendors, or external banks holding the contract to administer the Department's purchase card program.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored in electronic format. A description of standard Department of State policies concerning storage of electronic records is found at https://fam.state.gov/FAM/05FAM/05FAM0440.html.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: By individual name, address, telephone number, or email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are retired and destroyed in accordance with published Department of State Records Disposition Schedules as approved by the National Archives and Records Administration (NARA) and outlined at https://foia.state.gov/Learn/RecordsDisposition.aspx. The range of disposition for records maintained in the system is one to six years. More specific information may be obtained by writing to the following address: U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All Department of State network users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Department OpenNet network users are required to take

the Foreign Service Institute distance learning course instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly. Before being granted access to Integrated Logistics Management Records, a user must first be granted access to the Department of State computer network.

Department of State employees and contractors may remotely access this system of records using non-Department owned information technology. Such access is subject to approval by the Department's mobile and remote access program and is limited to information maintained in unclassified information systems. Remote access to the Department's information systems is configured in compliance with OMB Circular A-130 multifactor authentication requirements and includes a time-out function.

All Department of State employees and contractors with authorized access to records maintained in this system of records have undergone a thorough background security investigation. Access to the Department of State, its annexes, and posts abroad is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.

The safeguards in the following paragraphs apply only to records that are maintained in government-certified cloud systems. All cloud systems that provide IT services and process Department of State information must be specifically authorized by the Department of State Authorizing Official and Senior Agency Official for

Privacy.

Information that conforms with Department-specific definitions for Federal Information Security Modernization Act (FISMA) low, moderate, or high categorization are permissible for cloud usage and must specifically be authorized by the Department's Cloud Program Management Office and the Department of State Authorizing Official. Specific security measures and safeguards will depend on the FISMA categorization of the information in a given cloud system. In accordance with Department policy, systems that process more sensitive information will require more stringent controls and review by Department cybersecurity experts prior to approval. Prior to operation, all Cloud systems must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB regulations, National Institute of Standards and Technology's (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS) and Department of State policies and standards.

All data stored in cloud environments categorized above a low FISMA impact risk level must be encrypted at rest and in-transit using a federally-approved encryption mechanism. The encryption keys shall be generated, maintained, and controlled in a Department data center by the Department key management authority. Deviations from these encryption requirements must be approved in writing by the Department of State Authorizing Official. High FISMA impact risk level systems will additionally be subject to continual auditing and monitoring, multifactor authentication mechanism utilizing Public Key Infrastructure (PKI) and NIST 800 53 controls concerning virtualization, servers, storage and networking, as well as stringent measures to sanitize data from the cloud service once the contract is terminated.

RECORD ACCESS PROCEDURES: Individuals who wish to gain access to or

amend records pertaining to themselves should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520. The individual must specify that he or she wishes the Integrated Logistics Management Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Integrated Logistics Management Records include records pertaining to the individual. Detailed instructions on Department of State procedures for accessing and amending records can be found on the Department's FOIA website at https://foia.state.gov/Request/Guide.aspx.

CONTESTING RECORD PROCEDURES: Individuals who wish to contest record procedures should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520.

NOTIFICATION PROCEDURES: Individuals who have reason to believe that this system of records may contain information pertaining to them may write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520. The individual must specify that he/she wishes the Integrated Logistics Management Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of

the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Integrated Logistics Management Records include records pertaining to the individual.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: Previously published at 71 FR 8884.

Eric F. Stein,

Deputy Assistant Secretary,

Bureau of Administration,

Global Information Services,

US Department of State.

[FR Doc. 2022-01346 Filed: 1/24/2022 8:45 am; Publication Date: 1/25/2022]